

# **DETECTING COMPUTER VIRUSES OR MALICIOUS SOFTWARE BY PATCHING INSTRUCTIONS INTO AN EMULATOR**

## **ABSTRACT**

One embodiment of the present invention provides a system for emulating computer viruses and/or malicious software that operates by patching additional program instructions into an emulator in order to aid in detecting a computer virus and/or malicious software within suspect code. During operation, the system loads a first emulator extension into the emulator. This first emulator extension includes program instructions that aid in the process of emulating the suspect code in order to detect a computer virus and/or malicious software. The system also loads the suspect code into an emulator buffer. Next, the system performs an emulation using the first emulator extension and the suspect code. This emulation is performed within an insulated environment in a computer system so that the computer system is insulated from malicious actions of the suspect code. During this emulation, the system determines whether the suspect code is likely to exhibit malicious behavior. In one embodiment of the present invention, loading the first emulator extension into the emulator involves loading the first emulator extension into the emulator buffer within the emulator. In this embodiment, performing the emulation involves emulating the program instructions that comprise the first emulator extension.